BRM – For the new kid on the block

In line with my other documents ARA – For the new kid on the block, EAM – For the new kid on the block & ARM – For the new kid on the block this is the final installment of the four components that comprise GRC AC. The objective of this post is to help people who are new to this neck of the woods/Access Control, an overview of my understanding of what BRM is all about and how it works.

As usual feel free to skip it if you are well versed in this topic, however please do stick around and feel free to enlighten me with your expertise if I made any mistakes or if you would like to correct/add more on/to this topic.

Business Role Management (BRM)
This is same as PFCG in R/3 where you build a role. BRM is a web based application that automates the creation and management of Roles. Unlike in the backend system, BRM enforces best practices to ensure that the Role development, testing and maintenance is consistent across the entire implementation, resulting in lower ongoing maintenance and painless knowledge transfer. BRM provides Role Owners and Security Administrators with the means to create and maintain role definitions, identify potential audit and segregation of duties issues. It empowers them to document important role information that can be of great value for better role management. One key element of provisioning in BRM is the identification and mitigation of risks at an early stage, even before the creation of the roles. Risks can be identified as a conflict within a single role, composite role, derived role and templates respectively. This is done with the help of ARA, which provides means to quantify the risks associated with roles and suggests possible remediation and mitigation control procedure. Business Role concept is the new addition to ERM (5.3). Business roles are system independent, which means you can assign a technical role from one system and another from a different system. A bit like Composite roles but the difference is, roles are not restricted to one system. Although a Business role gets assigned to an end user, it will not be reflected in the backend system. All he/she will be provisioned is a group of technical roles that are associated with the Business Role.

Business Role Management (BRM)

The Nitty Gritty

Creating Roles through BRM, helps Security Admin and Role Owners in:

- Tracking progress during role implementation.
- Monitoring the overall quality of the role implementation.
- Performing risk analysis at role design phase.
- Providing an audit trail for all role modifications.
- Enable Firefighter roles for Firefighting
- Flexible role building workflows, which includes preventative simulations
- Maintaining roles after they are generated to keep role information current.
- Enforces Segregation of duties from the ground up by starting with clean role definitions
- Role Comparison to detect backend changes, which provides role consistency, synchronization, and compliance

For example, a person who has authorization to change HR Master Data, should not have authorization to change payroll information as well. If such a conflict action is found in a role, BRM proactively alerts the security team about the considered risk and hence a corrective measure can be established. BRM centralizes and standardizes enterprise wide role management, eliminating manual errors, providing an audit trail for changes, and enforcing user access best practices.

BRM allows to:

- Create/Change a role in/for multiple systems.
- Supports multiple landscapes – cross enterprise/cross platform
- Risk Analysis/Simulation/Mitigation
- Multiple Role comparison
- Mass Role Generate/import/update/RA
- Role Certification
- Transaction Usage Report

Key stages in Role Creation process through BRM:

- Role Definition: Enter the role details
- Authorization: This is where you assign T-Codes/Authorizations
- Risk Analysis: This is where you analyze risks through ARA
- Approval: This is where you integrate it with ARM for role assignment/provisioning through pre-configured workflows.

BRM Best Practices

- Design a good role naming convention.
- Well thought out integration of BRM into ongoing role development, testing and change management processes.
- Identify key users (e.g., Role Owners, Security Administrators, and User Administrators) and how they will use and customize BRM accordingly.
- Define goals (e.g: role optimization or consolidation, user access optimization, reducing risk, reducing the role change requests)
- Identify custom reports and attach them to BRM.

Linch.pin of BRM

Role Methodology

Business Role Management (BRM)

The Nitty Gritty

Creating Roles through BRM, helps Security Admin and Role Owners in:

- Tracking progress during role implementation.
- Monitoring the overall quality of the role implementation.
- Performing risk analysis at role design phase.
- Providing an audit trail for all role modifications.
- Enable Firefighter roles for Firefighting
- Flexible role building workflows, which includes preventative simulations
- Maintaining roles after they are generated to keep role information current.
- Enforces Segregation of duties from the ground up by starting with clean role definitions
- Role Comparison to detect backend changes, which provides role consistency, synchronization, and compliance

For example, a person who has authorization to change HR Master Data, should not have authorization to change payroll information as well. If such a conflict action is found in a role, BRM proactively alerts the security team about the considered risk and hence a corrective measure can be established. BRM centralizes and standardizes enterprise wide role management, eliminating manual errors, providing an audit trail for changes, and enforcing user access best practices.

This is where you define the methodology processes and steps for role maintenance. The application provides a set of actions that can be used for role maintenance, such as definition, risk analysis, generation. You can select which actions to use, the order and the frequency. For example, you can define that four steps are required to maintain a role and that approval is required after each step.

Defining a step

SAP provides a set of actions that you can perform for role maintenance. When you define a step, you select which actions to use and assign a name that is in line with your company guidelines. For example, you can select delivered Action and Permissions, and name its phase as Maintain Authorizations.

Defining a methodology process

You create the methodology process as a framework to attach the methodology steps. You can create as many methodology processes as needed. For example, you may want to have one methodology for finance role requests, and another for office administration role requests.

Adding steps to the methodology process

You assign the steps to the methodology process and select the order of the steps. For example, for finance role requests, you may want to require several approval steps and risk analysis.

Business Role Management (BRM)

The Nitty Gritty

Creating Roles through BRM, helps Security Admin and Role Owners in:

- Tracking progress during role implementation.
- Monitoring the overall quality of the role implementation.
- Performing risk analysis at role design phase.
- Providing an audit trail for all role modifications.
- Enable Firefighter roles for Firefighting
- Flexible role building workflows, which includes preventative simulations
- Maintaining roles after they are generated to keep role information current.
- Enforces Segregation of duties from the ground up by starting with clean role definitions
- Role Comparison to detect backend changes, which provides role consistency, synchronization, and compliance

For example, a person who has authorization to change HR Master Data, should not have authorization to change payroll information as well. If such a conflict action is found in a role, BRM proactively alerts the security team about the considered risk and hence a corrective measure can be established. BRM centralizes and standardizes enterprise wide role management, eliminating manual errors, providing an audit trail for changes, and enforcing user access best practices.

**** If you wish to create customized methodology processes, like conditioned based workflows and approvals; then you can incorporate MSMP workflows for automation of approvals and provisioning, using BRF+ to define conditions.***

Configuration in a Nutshell

1. Create all BRM users or decide amongst the existing users who gets what BRM role using ‘SU01’
2. Create/customize all BRM roles using ‘PFCG’
    - SAP_GRAC_ROLE_MGMT_ROLE_OWNER: Approver for Role Maintenance
3. Assign the roles to their respective users using ‘SU01’
4. Maintain GRC System Configuration Parameters:
    - SPRO -> IMG -> GRC -> AC-> Maintain Configuration Settings -> Role Management
5. Activate/Check following BC Sets using ‘SCPR20’
    - GRAC_ROLE_MGMT_LANDSCAPE
    - GRAC_ROLE_MGMT_METHODOLOGY
    - GRAC_ROLE_MGMT_PRE_REQ_TYPE
    - GRAC_ROLE_MGMT_ROLE_STATUS
    - GRAC_ROLE_MGMT_SENSITIVITY
    - GRC_MSMP_CONFIGURATION (Optional)
    - Maintain Connection Settings: ‘ROLMG’ Integration scenario
    - SPRO -> IMG -> GRC -> Common Component Settings -> Integration Framework -> Maintain Integration Scenario
    - Associate actions and assign default connectors:
    - SPRO -> IMG -> GRC -> AC-> Maintain Mapping for Actions and Connector Groups
        - 001 Role Generation
        - 002 Role Risk Analysis

Business Role Management (BRM)

Configuration in a Nutshell

  - 003 Authorization Maintenance
  - 004 Provisioning
  - 005 HR Triggers (optional)
- Maintain Role Type Settings: You can either activate/deactivate pre-delivered role types to suit your needs and set maximum length for the name of the role
- SPRO -> IMG -> GRC -> AC-> Role Management -> Maintain Role Type Settings
- Defining and manage Naming Conventions: This is where you can set a pre-defined naming convention for naming roles
- SPRO -> IMG -> GRC -> AC-> Role Management -> Specify Naming Convention
- Maintain Project and Product Release Name: These are the attributes that you can assign to roles.
- SPRO -> IMG -> GRC -> AC-> Role Management -> Maintain Project and Product Release Name
- Define Role Sensitivity: Sensitivity of role can be set here
- SPRO -> IMG -> GRC -> AC-> Role Management -> Define Role Sensitivity
- Maintain Role Status:Maintain status of the role here. Only roles with status Production are available for user role requests
- SPRO -> IMG -> GRC -> AC-> Role Management -> Maintain Role Status
- Specify Critical Level: Specify how essential a role is to the company
- SPRO -> IMG -> GRC -> AC-> Role Management -> Specify Critical Level
- Define Companies:
- SPRO -> IMG -> GRC -> AC-> Role Management -> Define Companies
- Maintain Functional Areas: Specify a group or department in a company that performs a specific task or function such as Accounting.
- SPRO -> IMG -> GRC -> AC-> Role Management -> Maintain Functional Areas
- Define Prerequisite Types: Define role prerequisites that are required to be validated before granting access to a user
- SPRO -> IMG -> GRC -> AC-> Role Management -> Define Prerequisite Types
- Define Role Prerequisites: Define prerequisites for a role to be assigned
- SPRO -> IMG -> GRC -> AC-> Role Management -> Define Role Prerequisites
- Maintain Business Processes and Sub Processes: Serves similar purpose as Functional Areas
- SPRO -> IMG -> GRC -> AC-> Maintain Business Process and Sub Processes
- Create/Maintain AC Owners
- NWBC -> Setup -> Access Owners -> Access Control Owners
- Assign Condition Groups to BRFplus Functions: You can assign two pre-delivered condition group types (methodology

Business Role Management (BRM)

Configuration in a Nutshell

and approver) to the BRFplus applications and the BRFplus functions.

- SPRO -> IMG -> GRC -> AC-> Role Management -> Assign Condition Groups to BRFplus Functions
- Define Methodology Processes and Steps:
- SPRO -> IMG -> GRC -> AC-> Role Management -> Define Methodology Process and Steps
- Associate Methodology Process to Condition Group: you can associate the methodology processes to a condition group. The application uses this association to determine which methodology process to use based on the specified settings in the condition group.
- SPRO -> IMG -> GRC -> AC-> Role Management -> Associate Methodology Process to Condition Group
- Generate BRF+ Rules (Optional)
- TCode: BRF+
- Maintain MSMP Workflows: This needs to be configured if there is an approval step in Role Creation Methodology

This pretty much is the gist of BRM and should be enough to get you started. For a more comprehensive understanding/configuration and other bits and pieces on this topic, please check out the links in the following document put together by ***Alessandro***, which covers everything in detail. Please check under Business Role Management (BRM).

http://scn.sap.com/docs/DOC-57438